CLAIMS

1. (PREVIOUSLY PRESENTED) A system for controlling access to digital services comprising:

(a) a control center configured to coordinate and provide digital services;

(b) an uplink center configured to receive the digital services from the control center and transmit the digital services to a satellite;

(c) the satellite configured to:

(i) receive the digital services from the uplink center;

(ii) process the digital services; and

(iii) transmit the digital services to a subscriber receiver station;

(d) the subscriber receiver station configured to:

(i) receive the digital services from the satellite;

(ii) control access to the digital services through an integrated receiver/decoder (IRD);

(e) a conditional access module (CAM) communicatively coupled to the IRD, wherein the CAM comprises:

(i) a protected nonvolatile memory component, wherein:

(1) the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services; and

(2) the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only; and

(3) access to the protected nonvolatile memory component is isolated;

(ii) a microprocessor's unprotected nonvolatile memory component wherein the microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same;

(iii) a hidden non-modifiable identification number embedded into the protected nonvolatile memory component, wherein:

(1) the identification number uniquely identifies the CAM; and

(2) the identification number is used to limit a cloning attack wherein said cloning attack comprises copying the identification number to a new CAM; and

(iv) a fixed state custom logic block, wherein the protected nonvolatile memory component is not directly accessible via a system bus and access to the protected nonvolatile memory component is limited to the custom logic block, and wherein data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block.

2. (PREVIOUSLY PRESENTED) The system of claim 1 wherein the protected nonvolatile memory component is isolated such that a system input/output module, microprocessor, or external environment is prevented from direct access to the identification number.

3. (ORIGINAL) The system of claim 1 wherein the identification number is embedded after manufacturing.

4. (ORIGINAL) The system of claim 1 wherein the custom logic block is permitted to read the identification number.

5. (ORIGINAL) The system of claim 4 wherein a function defined in the custom logic block specifies an operation to be performed using the hidden identification number.

6. (PREVIOUSLY PRESENTED) The system of claim 1 further comprising a onetime programmable memory protected by a hardware fuse that isolates the identification number from a microprocessor after the identification number is written.

7. (PREVIOUSLY PRESENTED) The system of claim 1 wherein the custom logic block is configured to embed the identification number into the protected nonvolatile memory component.

8. (PREVIOUSLY PRESENTED) The system of claim 1 further comprising a microprocessor that is configured to embed the identification number into the protected nonvolatile memory component.

9. (ORIGINAL) The system of claim 1 wherein access to the digital services is rejected when the hidden non-modifiable identification number is on a list of unauthorized identification numbers.

10. (PREVIOUSLY PRESENTED) A method for limiting unauthorized access to digital services comprising:

(a) embedding a hidden non-modifiable identification number into a protected nonvolatile memory component, wherein:

(i) the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services;

(ii) the hidden non-modifiable identification number uniquely identifies a device containing the protected nonvolatile memory component;

(iii) access to the digital services is based on access rights associated with the hidden non-modifiable identification number; and

(iv) the identification number is used to limit a cloning attack wherein said cloning attack comprises copying the identification number to a new device; and

(b) isolating access to the protected nonvolatile memory component wherein:

(i) access to the protected nonvolatile memory component is limited to a fixed state custom logic block;

(ii) the protected nonvolatile memory component is protected such that the protected nonvolatile memory component is read only;

(iii) the protected nonvolatile memory component is not directly accessible via a system bus;

(iv) data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block; and

(v) a microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same.

11. (PREVIOUSLY PRESENTED) The method of claim 10 wherein the protected nonvolatile memory component is isolated by preventing a system input/output module, microprocessor, or external environment from direct access to the identification number.

12. (ORIGINAL) The method of claim 10 wherein the identification number is embedded after manufacturing.

13. (ORIGINAL) The method of claim 10 wherein the custom logic block is permitted to read the identification number.

14. (ORIGINAL) The method of claim 13 wherein a function defined in the custom logic block specifies an operation to be performed using the hidden identification number.

15. (PREVIOUSLY PRESENTED) The method of claim 10 wherein the identification number is embedded using a onetime programmable memory protected by a hardware fuse that isolates the identification number from a microprocessor after the identification number is written.

16. (PREVIOUSLY PRESENTED) The method of claim 10 wherein the custom logic block embeds the identification number into the protected nonvolatile memory component.

17. (PREVIOUSLY PRESENTED) The method of claim 10 wherein a microprocessor embeds the identification number into the protected nonvolatile memory component.

18. (ORIGINAL) The method of claim 10 further comprising rejecting access to the digital services when the hidden non-modifiable identification number is on a list of unauthorized identification numbers.

19. (PREVIOUSLY PRESENTED) A conditional access module (CAM), comprising:

(a) a microprocessor;

(b) an un-protected nonvolatile memory component connected to the microprocessor;

(c) a protected nonvolatile memory component, wherein:

(i) the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing digital services; and

(ii) the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only; and

(iii) access to the protected nonvolatile memory component is isolated;

(iv) the unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same;

(b) a hidden non-modifiable identification number embedded into the protected nonvolatile memory component, wherein:

(i) the identification number uniquely identifies the CAM; and

(ii) the identification number is used to limit a cloning attack wherein said cloning attack comprises copying the identification number to a new CAM; and

(c) a fixed state custom logic block, wherein the protected nonvolatile memory component is not directly accessible via a system bus and access to the protected nonvolatile memory component is limited to the custom logic block, and wherein data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block.

20. (PREVIOUSLY PRESENTED) The CAM of claim 19 wherein the protected nonvolatile memory component is isolated such that a system input/output module, microprocessor, or external environment is prevented from direct access to the identification number.

21. (ORIGINAL) The CAM of claim 19 wherein the identification number is embedded after manufacturing.

22. (ORIGINAL) The CAM of claim 19 wherein the custom logic block is permitted to read the identification number.

23. (ORIGINAL) The CAM of claim 22 wherein a function defined in the custom logic block specifies an operation to be performed using the hidden identification number.

24. (PREVIOUSLY PRESENTED) The CAM of claim 19 further comprising a onetime programmable memory protected by a hardware fuse that isolates the identification number from the microprocessor after the identification number is written.

25. (PREVIOUSLY PRESENTED) The CAM of claim 19 wherein the custom logic block is configured to embed the identification number into the protected nonvolatile memory component.

26. (PREVIOUSLY PRESENTED) The CAM of claim 19 wherein the microprocessor is configured to embed the identification number into the protected nonvolatile memory component.

27. (ORIGINAL) The CAM of claim 19 wherein access to the digital services is rejected when the hidden non-modifiable identification number is on a list of unauthorized identification numbers.

28. (PREVIOUSLY PRESENTED) An article of manufacture for limiting unauthorized access to digital services comprising:

(a) means for embedding a hidden non-modifiable identification number into a protected nonvolatile memory component, wherein:

(i) the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services;

(ii) the hidden non-modifiable identification number uniquely identifies a device containing the protected nonvolatile memory component;

(iii) access to the digital services is based on access rights associated with the hidden non-modifiable identification number; and

(iv) the identification number is used to limit a cloning attack wherein said cloning attack comprises copying the identification number to a new device; and

(b) means for isolating access to the protected nonvolatile memory component wherein:

(i) access to the identification number is limited to a fixed state custom logic block;

(ii) the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only;

(iii) the protected nonvolatile memory component is not directly accessible via a system bus;

(iv) data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block; and

(v) a microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same.

29. (PREVIOUSLY PRESENTED) The article of manufacture of claim 28 wherein the protected nonvolatile memory component is isolated by preventing a system input/output module, microprocessor, or external environment from direct access to the identification number.

30. (ORIGINAL) The article of manufacture of claim 28 wherein the identification number is embedded after manufacturing.

31. (ORIGINAL) The article of manufacture of claim 28 wherein the custom logic block is permitted to read the identification number.

32. (ORIGINAL) The article of manufacture of claim 31 wherein a function defined in the custom logic block specifies an operation to be performed using the hidden identification number.

33. (PREVIOUSLY PRESENTED) The article of manufacture of claim 28 wherein the identification number is embedded using a onetime programmable memory protected by a hardware fuse that isolates the identification number from the microprocessor after the identification number is written.

34. (PREVIOUSLY PRESENTED) The article of manufacture of claim 28 wherein the custom logic block embeds the identification number into the protected nonvolatile memory component.

35. (PREVIOUSLY PRESENTED) The article of manufacture of claim 28 wherein the microprocessor embeds the identification number into the protected nonvolatile memory component.

36. (ORIGINAL) The article of manufacture of claim 28 further comprising means for rejecting access to the digital services when the hidden non-modifiable identification number is on a list of unauthorized identification numbers.